PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 07 March 2000 (07.03.00)	
International application No. PCT/CA99/00560	**Applicant's or agent's file reference** 08-883817WO
International filing date (day/month/year) 18 June 1999 (18.06.99)	**Priority date** (day/month/year) 18 June 1998 (18.06.98)
Applicant AHMADI, Babak et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

17 January 2000 (17.01.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Juan Cruz
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

SECHLEY, Konrad, A.
Gowling Lafleur Henderson LLP
Suite 2600
160 Elgin Street
Ottawa, Ontario K1P 1C3
CANADA

Date of mailing (day/month/year)
14 August 2000 (14.08.00)

Applicant's or agent's file reference
08-883817WO

IMPORTANT NOTIFICATION

International application No.
PCT/CA99/00560

International filing date (day/month/year)
18 June 1999 (18.06.99)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address
SECHLEY, Konrad, A.
Gowling, Strathy & Henderson
Suite 2600
160 Elgin Street
Ottawa, Ontario K1P 1C3
Canada

State of Nationality:
State of Residence:
Telephone No.: 613 233 1781
Facsimile No.: 613 563 9869
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
SECHLEY, Konrad, A.
Gowling Lafleur Henderson LLP
Suite 2600
160 Elgin Street
Ottawa, Ontario K1P 1C3
Canada

State of Nationality:
State of Residence:
Telephone No.: 613 233 1781
Facsimile No.: 613 563 9869
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
A. Karkachi

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREA

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
08-883817WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/CA 99/ 00560	18/06/1999	18/06/1998
Applicant		
AHMADI, Babak et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [ ] the text is approved as submitted by the applicant.

   [X] the text has been established by this Authority to read as follows:

   BAIT SOFTWARE

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. _____

   [ ] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [X] None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
CT/CA 99/00560

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 94 07204 A (R. RICHARDSON) 31 March 1994 (1994-03-31) page 1, line 8 -page 10, line 10 page 12, line 6 -page 23, line 9; claims; figures 1-8	1-3,11
A	EP 0 679 980 A (I. B. M.) 2 November 1995 (1995-11-02) column 8, line 47 -column 17, line 56; figure 15	1,5,9
A	US 5 291 598 A (GRUNDY) 1 March 1994 (1994-03-01) column 1, line 16 -column 6, line 23; claim 1; figure 1A	1-3,11

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 October 1999	20/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Soler, J

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 99/00560

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9407204 A	31-03-1994	AU 678985 B	19-06-1997
		AU 4811393 A	12-04-1994
		CA 2145068 A	31-03-1994
		CN 1103186 A	31-05-1995
		EP 0689697 A	03-01-1996
		NZ 255971 A	26-05-1997
		US 5490216 A	06-02-1996
EP 679980 A	02-11-1995	US 5757907 A	26-05-1998
		BR 9501522 A	21-11-1995
		CA 2145926 A,C	26-10-1995
		JP 7295801 A	10-11-1995
US 5291598 A	01-03-1994	US 5375240 A	20-12-1994

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT / CA 99/00560
International Application No.

18 JUNE 1999 (18.06.99)
International Filing Date

RO/CA
Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference
(if desired) (12 characters maximum) **O8-883817WO**

Box No. I TITLE OF INVENTION

Baitware

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

AHMADI, Babak
2322 Lawson Avenue
West Vancouver, British Columbia
CANADA V7V 2S6

☒ This person is also inventor.

Telephone No.
(604) 872-8588

Facsimile No.
(604) 872-8598

Teleprinter No.

State (that is, *country*) of nationality:
CA

State (that is, *country*) of residence:
CA

This person is applicant for the purposes of: ☒ all designated states ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

WIMMER, Carl P.
9 West Broadway
Vancouver, British Columbia
CANADA V5Y 1P1

This person is:
☐ applicant only
☒ applicant and inventor
☐ inventor only (*If this check-box is marked, do not fill in below.*)

State (that is, *country*) of nationality:
CA

State (*that is, country*) of residence:
CA

This person is applicant for the purposes of: ☒ all designated states ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

SECHLEY, Konrad A.; ERRATT, Judy A.; D'IORIO, Helene; ROSS, John W.; MORGAN, Bruce E.; DUDLEY, Bruce; STRAZNICKY, Ivan; O'NEILL, T. Gary; WADA, Ikuko
Gowling, Strathy & Henderson
Suite 2600, 160 Elgin Street
Ottawa, Ontario
Canada K1P 1C3

Telephone No.
(613) 233-1781

Facsimile No.
(613) 563-9869

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

RO/CA

Box No. V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) (*mark the applicable check-boxes; at least one must be marked*):

Regional Patent

☐ **AP** **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudan, SZ Swaziland, UG Uganda, ZW Zimbabwe and any other State which is a Contracting State of the Harare Protocol and of the PCT

☐ **EA** **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ **EP** **European Patent:** AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☐ **OA** **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senagal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (*if other kind of protection or treatment desired, specify on dotted line*).....

National Patent (*if other kind of protection or treatment desired, specify on dotted line*):

- ☐ **AE** United Arab Emirates.....
- ☐ **AL** Albania.....
- ☐ **AM** Armenia.....
- ☐ **AT** Austria .....
- ☐ **AU** Australia.....
- ☐ **AZ** Azerbaijan
- ☐ **BA** Bosnia and Herzegovina
- ☐ **BB** Barbados
- ☐ **BG** Bulgaria .....
- ☐ **BR** Brazil .....
- ☐ **BY** Belarus
- ☒ **CA** Canada
- ☐ **CH and LI** Switzerland and Liechtenstein
- ☐ **CN** China .....
- ☐ **CU** Cuba .....
- ☐ **CZ** Czech Republic .....
- ☐ **DE** Germany .....
- ☐ **DK** Denmark .....
- ☐ **EE** Estonia .....
- ☐ **ES** Spain .....
- ☐ **FI** Finland .....
- ☐ **GB** United Kingdom
- ☐ **GD** Grenada
- ☐ **GE** Georgia.....
- ☐ **GH** Ghana .....
- ☐ **GM** Gambia .....
- ☐ **HR** Croatia
- ☐ **HU** Hungary.....
- ☐ **ID** Indonesia
- ☐ **IL** Israel .....
- ☐ **IN** India .....
- ☐ **IS** Iceland
- ☒ **JP** Japan .....
- ☐ **KE** Kenya .....
- ☐ **KG** Kyrgyzstan .....
- ☐ **KP** Democratic People's Republic of Korea .....
- ☐ **KR** Republic of Korea .....
- ☐ **KZ** Kazakstan .....
- ☐ **LC** Saint Lucia
- ☐ **LK** Sri Lanka
- ☐ **LR** Liberia
- ☐ **LS** Lesotho .....
- ☐ **LT** Lithuania
- ☐ **LU** Luxembourg .....
- ☐ **LV** Latvia
- ☐ **MD** Republic of Moldova .....
- ☐ **MG** Madagascar .....
- ☐ **MK** The former Yugoslav Republic of Macedonia .....
- ☐ **MN** Mongolia
- ☐ **MW** Malawi .....
- ☐ **MX** Mexico .....
- ☐ **NO** Norway
- ☐ **NZ** New Zealand .....
- ☐ **PL** Poland .....
- ☐ **PT** Portugal .....
- ☐ **RO** Romania .....
- ☐ **RU** Russian Federation .....
- ☐ **SD** Sudan
- ☐ **SE** Sweden
- ☐ **SG** Singapore
- ☐ **SI** Slovenia .....
- ☐ **SK** Slovakia .....
- ☐ **SL** Sierra Leone
- ☐ **TJ** Tajikistan .....
- ☐ **TM** Turkmenistan .....
- ☐ **TR** Turkey .....
- ☐ **TT** Trinidad and Tobago .....
- ☐ **UA** Ukraine .....
- ☐ **UG** Uganda .....
- ☒ **US** United States of America .....
- ☐ **UZ** Uzbekistan .....
- ☐ **VN** Viet Nam .....
- ☐ **YU** Yugoslavia.....
- ☐ **ZA** South Africa
- ☐ **ZW** Zimbabwe

Check-boxes reserved for designating States (for the purposes of a national patent) which have become party to the PCT after issuance of this sheet:

- ☐ .....
- ☐ .....

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (*Confirmation of a designation consists of the filing of a notice specifying that designation and the payment of the designation and confirmation fees. Confirmation must reach the receiving office within the 15-month time limit.*)

Box No. VI PRIORITY CLA ☐ Further priority claims are indicated in the Supplemental Box

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application country	regional application:* regional Office	international application: receiving Office
item (1) 18 June 1998 (18.06.1998)	60/089,772	US		
item (2)				
item (3)				

☐ The receiving Office is hereby requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (*only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office*) identified above as item(s): _____

* *Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):* ISA / EP

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority):*

Date (*day/month/year*) Number Country (or regional Office)

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	:	3
description (excluding sequence listing part)	:	27
claims	:	4
abstract	:	1
drawings	:	12
sequence listing part of description	:	
Total number of sheets	:	47

This international application is **accompanied** by the item(s) marked below:

1. ☐ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganisms or other biological material
8. ☐ nucleoitide and/or amino acid sequence listing in computer readable form
9. ☐ other (*specify*):

Figure of the drawings which should accompany the abstract: 2

Language of filing of the international application: ENGLISH

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Konrad A. Sechley
Patent Agent

For receiving Office use only

1. Date of actual receipt of the purported international application: 18 JUNE 1999 (18.06.99)
2. Drawings:
   - ☒ received:
   - ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:
4. Date of timely receipt of the required corrections under PCT Article 11(2):
5. International Searching Authority specified by the applicant: ISA /
6. ☒ Transmittal of search copy delayed until search fee is paid

For International Bureau use only

Date of receipt of the record copy by the International Bureau:

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
08-883817WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/CA99/00560	18/06/1999	18/06/1998
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant AHMADI, Babak et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 8 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
17/01/2000	29.09.2000
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Van de Maele, L Telephone No. +49 89 2399 8805

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/CA99/00560

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-27 as originally filed

Claims, No.:

1-11 as originally filed

Drawings, sheets:

1/12-12/12 as originally filed

2. The amendments have resulted in the cancellation of:

☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-11
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-11
Industrial applicability (IA)	Yes:	Claims	
	No:	Claims	1-11

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Cited documents:

D1: WO 94 07204 (R. Richardson)
D2: EP 0 679 980 A (IBM)
D3: Us 5 291 598 A (GRUNDY)

ANNEX TO SECTIONS V AND VIII

1. The present application relates to a method for detecting and inhibiting illegal use of software. It proposes an enhancement of the already existing BurnIn protection method. This BurnIn method basically embeds protective software modules at installation time in the executable software. These modules can disable the software when certain conditions (e.g. expiration of a trial period) are met.

   The enhancement of the present proposed solution is to embed a further module in the executable software (page 21, line 18 ff.). This module offers a free upgrade of the already installed software to the user. This offer serves as a bait because it requires connecting to a server controlled by the software developer and thus allows the latter to verify the legality of the installed copy. This verification is based on a RID (registration id), which identifies the software copy, and a MIV (Machine Identifier Value), which identifies the user and the machine. Matching MIV-RID couples, corresponding to registered users, are stored in a database on the server. The free upgrade module will dynamically reconstruct the MIV on the user's PC and sent it together with the (in the executable software embedded) RID to the server. Comparing these MIV-RID couples from the user's PC with the couples stored on the server allows to identify an illegal copies, i.e. not installed on the computer of the registered user, and allows to activate/install software modules which will disable the illegal copy as embedded in these modules.

2. This particular concept of protecting software against piracy is not taught by the available prior art documents. None of the 3 prior art documents cited in the International Search Report (D1 - D3) discloses a solution which is also based on such MIV/RID pair. D1 and D3 do disclose the use of a MIV value, however not of

a separate RID value. They do refer to a RID similar value, however this value is integrated in the MIV.

Furthermore, none of these documents even remotely refers to a "bait" module, which tempts the user to connect to the registration server even when an already running full version of the software is on the local PC.

Therefore, a claim based on a concept as discussed in point 1 above would apparently meet the criteria of *Article 33 PCT*.

3. However, none of the present claims however meets the criteria of *Article 6 PCT*, for the reasons set out in points 4 to 9 below. Therefore, no positive statement in respect of *Article 33 PCT* can be made for any of these claims.

4 All claims only include method features. Therefore, their subject should be restricted to a method and not to a method and means as is at present the case.

5 **Claim 1**

5.a The following features of **claim 1** are not clearly and/or completely defined:

- it is not clear how the BurnIn process disables the software program after expiration of the trial period (point a.i);
- there is no definition of $D_{(x)}$, and $T_{(u)}$ (point a.ii);
- the generation of the MIV value is defined as "dynamically" (point a.iii). It is not clear in what respect this attribute is required because a definition without it would implicitly not be different;
- there is no definition of RID (point a.iv);
- there is no definition with respect to the generation/retrieval of the MIV and RID values at the user's PC during the initialization steps of the free upgrading. The Customer Database generated according to the definition in point d include all registered MIV/RID pairs. This Customer Database corresponds to the list of MIV's recorded on the CD as explained on page 13, lines 2 to 3 of the description. The description further indicates that the actual MIV of the user's PC must be calculated for comparing with the MIV's on that list. However, **claim 1** appears to be missing any features of such calculation;

- there is no clear definition in point g how the copy is disabled. More in particular, it is not indicated how the executable referred to in g.i arrives on the user's PC. According to the description (page 19, lines 9 ff.) this is based on software modules embedded in the software at installation time.

These clarity objections are not considered serious because they can easily be met with appropriate amendments based on the description. An correspondingly amended **claim 1** would apparently meet the requirements of *Article 33 PCT*.

5.b It appears however that the scope of protection offered by such an amended **claim 1** is unnecessarily restricted.

These restriction do not result from the amendments to overcome the clarity objections but mainly from the many BurnIn specific features already included in point a of **claim 1**. According to this point a, the installation is restricted to a trial period. The description (page 3, point A) however refers to an installation which, as an alternative, also allows a number of initial accesses. Furthermore, the description (page 12, line 16 to page 12, line 12) even refers to an installation without trial phase whereby the user is not forced but is baited to connect to the registration server by the offering of a free upgrade.

It is strongly suggested, in the applicants interest, to exclude as many features as possible from **claim 1** in order to get a wider scope of protection. The summary in point 1 above of what is considered to be the concept of the invention can be used as a guidance. The removed features can be filed in dependent claims. To avoid however that the amendments extend the subject-matter beyond the application as originally filed the applicant should identify those parts of the description which serve as a basis for such amendment. The previous paragraph already includes identification of certain relevant sections of the description in this respect.

6. **Claim 2**

Claim 2 appears to be only different from **claim 1** in that it relates to distribution and re-distribution rather than distribution and upgrading of software. **Claim 1** however includes features explicitly relating to such upgrading. Therefore, a mere reference to the method steps of **claim 1** cannot be used and thus present **claim**

2 lacks of clarity (*Article 6 PCT*). As an alternative, **claim 1** could be amended to relate to upgrading as well as re-distribution.

It is suggested to file an amended **claim 2** which repeats the features of **claim 1**, at the exception of those features which relate to software upgrading which should be reworded in terms of software re-distribution.

7. **Claims 3, 4, 7, 8, 10 and 11**

These claims merely define the claimed subject-matter in terms of the desired result without giving any technical features of a solution to achieve that result. Therefore, these claims do not meet the requirements of *Article 6 PCT*.

Furthermore, these are all independent claims. Therefore, amending these claims to overcome the clarity objection that they are lacking technical features would result in a new and different clarity objection. Namely, lack of clarity of the claims as a whole would arise, since the plurality of independent claims would make it difficult, if not impossible, to determine the matter for which protection is sought, and places an undue burden on others seeking to establish the extent of the protection.

Therefore, the applicant these claims should have been deleted.

8. **Claims 5 and 6**

The features of these claims do not solve the clarity problem of **claim 1**. Therefore also these claims do not meet the requirements of *Article 6 PCT*. However, they could have been maintained as dependent claims of an amended **claim 1**.

9. **Claim 9**

This claim relates to the case in which an installed software program is copied from one PC onto another whereby appropriate amendment of the registry are made on the second PC. This claim however merely defines the result to be obtained. Furthermore, this result is anyway automatically obtained when the installation on the first PC is made with a method as defined in **claim 1**. Therefore, this claim does not include any new technical features not yet defined

claim 1 and thus creates an unjustified impression of being a further embodiment. Therefore this claim obscures the clarity of the claims and should be deleted, *Article 6 PCT*.

ANNEX TO SECTION VII

1. Contrary to the requirements of *Rule 5.1(a)(ii) PCT*, the relevant background art disclosed in document **D1**, which is considered to be the closest prior art document, is not mentioned in the description, nor is this document identified therein.

2. The independent claims are not drafted in the two-part form in accordance with *Rule 6.3(b) PCT* with those features known in combination from the prior art document **D1** being placed in the preamble (*Rule 6.3(b)(i) PCT*) and with the remaining features being included in the characterising part (*Rule 6.3(b)(ii) PCT*).

3. In case the applicant files an amended set of claims in a subsequent national phase, then he/she should at the same time make the description conform with amended claims.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 1/00

A1

(11) International Publication Number: WO 99/66386

(43) International Publication Date: 23 December 1999 (23.12.99)

(21) International Application Number: PCT/CA99/00560

(22) International Filing Date: 18 June 1999 (18.06.99)

(30) Priority Data:
60/089,772 18 June 1998 (18.06.98) US

(71)(72) Applicants and Inventors: AHMADI, Babak [CA/CA]; 2322 Lawson Avenue, West Vancouver, British Columbia V7V 2S6 (CA). WIMMER, Carl, P. [CA/CA]; 9 West Broadway, Vancouver, British Columbia V5Y 1P1 (CA).

(74) Agents: SECHLEY, Konrad, A. et al.; Gowling, Strathy & Henderson, Suite 2600, 160 Elgin Street, Ottawa, Ontario K1P 1C3 (CA).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: BAIT SOFTWARE

(57) Abstract

The present invention affords a software developer the ability to influence and/or control a copy of an application after he has lost physical possession of that copy. Baitware enables this through the inclusion of one or more features whose inclusion or removal, whose activation or subsequent deactivation are absolutely denied to the end user. Baitware extends this protection through a multilayer set of requirements, including fixing the copy of the application to one or more specific machines, registering this information at a remote server and subsequently transmitting to valid users only the correct keys to activate or deactivate usage blocking features.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

BAIT SOFTWARE

The present invention relates to software piracy. More specifically, the present invention relates to a method for the restriction or prevention of software piracy.

BACKGROUND OF THE INVENTION

The problem of software piracy arises from the nature of software itself, in that any copy of software is a binary copy, a perfect copy that will run the same as the original. In fact, the only thing distinguishing two binary copies of any software is their respective locations in time and space. Therefore the relapse of one unprotected copy of any program opens up the possibility of an infinite number of copies being made.

Any user can infringe the copyright of almost any software without any chance of being noticed or caught as long as his machine is not physically examined for pirated software.

Software piracy represents an enormous revenue loss for every software developer, which loss can be a multiple of the actual earned revenue of that developer. This invention enables the software developer to restrict or prevent software piracy.

Several devices and methods have been introduced over time to limit or constrain software piracy but they all fail in some important and logical manner to absolutely prevent piracy. Piracy must be prevented in an absolute manner since the release out of the hands of the developer of even one unprotected copy, permits endless copying and distribution by hackers, infringers and pirates.

There are many TrialWare products (such as TimeLock) which allow an application developer to distribute a demo or trial version of his software which "expires" on the user's computer after a set number of accesses or a set period of time. The problem occurs after the user has paid a fee and "unlocked" the software so that it becomes fully functional.

At that point, the software can be distributed to infringers by copying the installed program. There may be changes required to the setup or Registry of the infringers computer to incorporate certain setup or enabling features but a semi-skilled hacker can accomplish this. In fact, the Warez sites on the Internet are places where unprotected copies of many products can be downloaded. The "Hacking" of the protection features of TrialWare products is a game for certain people and status in that forum is gained by the number and complexity of protected programs which have been hacked and re-released as "freeware".

Baitware works by including multiple levels of protection.

A At the front end, Baitware employs trialware features (limiting the initial time or the number of initial accesses - to be set by the developer) to encourage the user to register the installation of the application.

B Upon registration, the RID (Registration Identifier) server can use the MIV (Machine Identifier Value) of the user to calculate an unlock code which will only unlock that single copy of the application as already installed on the valid (paid) users system.

C Upon registration, the RID server now has the contact information required to ensure that only one copy of each valid and paid RID is installed, preventing multiple installation of a single copy

D The RID server now has a complete list of each valid user, to whom will be sent, from time to time, special codes to unlock or deactivate the buried features, which are the fallback defense of Baitware should the front end defenses ever fail.

These fallback defenses are not known to the users in advance and may include multiple, cascading drop dead dates which freeze the application further use and invite the infringer to contact customer service for registration. Drastic action such as overwriting portions of the EXE in some random fashion which would totally disable further use, are also possible.

E If desired, the RID server can be set to receive information sent at discrete intervals by any installed application, whether valid or not.

The transmission of this information would be invisible to the user and would inform the RID server that infringement has taken place, and give the email address of the infringer.

What this application discloses and teaches is a safe method for the developer to supply an antidote to the legal users while preventing infringers from taking that antidote under any circumstances.

It is an object of the invention to overcome disadvantages of the prior art.

The above object is met by the combination of features of the main claim, the sub-claims disclose further advantageous embodiments of the invention.

SUMMARY OF THE INVENTION

The present invention relates to the restriction or prevention of software piracy.

According to the present invention there is provided a method and means of preventing software piracy comprising the steps of:

a.)Treating the software to use the Burnin process, wherein Burnin performs the initialization steps of:

i.)Calculating a trial period ($T_{(x)}$) from first execution, after which the program becomes expired, whereby expired programs are disabled via Burnin depending on software developer preference,

ii.)Assigning an undisclosed "absolute expiry date" or death-date, $D_{(d)}$, set for a date which is given by:

$D_{(d)} = D_{(x)} + T_{(d)}$, where $T_{(d)}$ is a time period of at least 3 times the time period $T_{(u)}$

iii.)Dynamically generating an MIV value using the current computer software and hardware configurations,

iv.)Prompting the user for user information and the developer supplied RID, where the set of user information is specified by the software developer,

v.)Recording all data from steps i-iv in random and developer-specified locations in the executable file for the software,

vi.)Recording all data from steps i-iv in random and developer-specified locations within the current system-configuration-definition or registry,

b.)Distributing the BurnIned software in version $V_{(x)}$ as TrialWare on the date $D_{(x)}$ via any and all distribution channels, these channels including:

i.)Floppies

ii.) CD-ROM

iii.) Internet

iv.) Intranet

v.)Extranet

c.)Generating and dispensing a new and unique RID value for each copy of software sold to a user, the RID value being unique across all versions of the software throughout its life-time,

d.)Augmenting the Burnin process with a new step to re-cover user-registration data for paid users, including the MIV and RID values, from all installations and/or first-executions of the software, and to further store this data in the Customer Database,

e.)Constructing a free upgrade of the software in version $V_{(x+1)}$ which includes the Customer Database constructed in step d; version $V_{(x+1)}$ being able to upgrade legal and illegal copies of the software in version $V_{(x)}$ via the initialization steps of:

i.)Searching the Customer Database for a matching MIV-RID pair,

ii.)If found, resetting the absolute expiry date, $D_{(x)}$, to Y years from current date, where Y is defined as the life-time of the software in version $V_{(x-1)}$,

iii.)If not found, recording all registration data and dynamically generated data to the central data base of step d, identifying a particular MIV as an illegal, but still upgraded user,

f.)Distributing the software in version $V_{(x-1)}$ constructed in step-e as a free upgrade within a time period, $T_{(u)}$, after the release date, $D_{(x)}$, where $T_{(u)}$ is specified by the software developer as the time period required for the product to reach 100% of currently legal users.

g.)Disabling each copy of the software in version $V_{(x-1)}$ on the death date $D_{(d)}$; this process, which is activated the next time the software is run on or after the death date, comprising the steps of:

i.)Executing and/or undertaking all additional actions specified by the software developer,

ii.)Further disabling the software in version $V_{(x)}$, thereby also disabling any future re-installations of the software in version $V_{(x)}$,

h.)Contacting all illegal users recorded in the Customer Database on the death date $D_{(d)}$, and communicating all software developer specified information.

þ

This summary of the invention does not necessarily describe all necessary features of the invention but that the invention may also reside in a sub-combination of the described features.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the invention will become more apparent from the following description in which reference is made to the appended drawings wherein:

FIGURE1 shows an embodiment of ann aspect of the present invention. This figure shows a computer 100, and the Baitware software 104, acting on any number of software applications 102, within the computer.

FIGURE 2 shows an aspect of th present invention indicating the basic components of the system described hererin.

FIGURE 3 shows another aspect of the present invention, and indicates the Lockdef record.

FIGURE 4 shows another aspect of the present invention, and indicates the Program Control Block (PCB), Registry Control Record (RCR), Time Lock Type (TLT) constants for LockDef.type, and Time Lock Action (TLA) constants for LockDef.action.

FIGURE 5 shows another aspect of the present invention, and indicates the data elements duplicated in the PCB and RCR.

FIGURE 6 shows another aspect of the present invention, and indicates the assocaitions of each program file in the system of the present invention.

FIGURE 7 shows another aspect of the present invention, and indicates the rquired Baitware development.

FIGURE 8 shows another aspect of the present invention, and indicates the setup of the Burlin module.

FIGURE 9 shows another aspect of the present invention, and indicates the functions carried out by Burnlin.

FIGURE 10 shows another aspect of the present invention, and indicates fall back defenses as described hererin.

FIGURE 11 shows another aspect of the present invention, and indicates the errors which may occur in the Baitware system.

FIGURE 12 shows another aspect of the present invention, and indicates the steps for Baitware operation with softwarre downloaded from the Internet.

DESCRIPTION OF PREFERRED EMBODIMENT

The present invention relates to software piracy. More specifically, the present invention relates to a method for the restriction or prevention of software piracy.

The following description is of a preferred embodiment by way of example only and without limitation to the combination of features necessary for carrying the invention into effect.

Components & Concepts

The Baitware method.

The first step is to bind the application directly to the machine. Using a product such as BurnIn, the first step is to mate a software program irrevocably to a specific machine. under the BurnIn system, the user inputs certain personal data as well as corporate data into a form at the first install. This information together certain configuration of the users machine creates a Machine Identifier Value (MIV).

BurnIn furthers the process by "branding" this information directly into the executable of the program at the first installation. Once the information which has been burned into the program is encrypted and randomly placed in the .EXE, the end user or any hacker should not be able to find, let alone alter the inserted information. There are alternative for providing machine information. For

example, every Intel CPU has a unique identifier that can be used at the first install to create the unique reference point.

At this point, at every activation of the program, the program will run out and test that the machine on which it is installed is the one which has the unique (and not user definable) identifier. If the response is correct, the application will run, if not, then not.

Using commonly available devices (such as telephone, email, fax, on-line) the end user is prompted to return the new MIV information together with the rest of the information in the form to the application developer. The developer may require this information as part of the registration process. To increase the difficulty of decrypting the essential Baitware information, blocks of meaningless data can also be included at random locations in the EXE to further increase the difficulty.

The specific copy of the application which has been installed is now fixed to a known system, The RID server will prevent further installation of that same identified copy to another machine. Should the user break through the defenses that prevent the copying of an already installed application or the installation of a copy without final authorization from the RID server, the fall back defenses will be required to come into play.

At some point, the developer releases an upgrade. This can be either on-line (freely downloadable) or on a CD-ROM. On that CD-ROM or download will be a list of Legal Users Names and Legal MIVs. The CD-ROM will check the actual MIV of the machine and regardless of whether the application being upgraded is legal or not, it will accomplish the upgrades without disruption. But only in the case of a legal copy (which is verified at upgrade time by searching for and verifying the MIV) will the fall back defences such as a secret drop-dead date be disabled.

This method causes every user (legal and otherwise) to swallow and ingest an application that has been baitwared, in effect, the user has swallowed a time bomb, which he cannot discover and cannot eliminate. Only the developer can eliminate or nullify the fallback defenses, by offer the antidote to the Baitware poison.

A crucial feature of this system is the delay before the fall back defenses activate. This time is developer specified and will depend on his preferences and knowledge of his own customer base. The central feature of this delay is that potential infringers will create data which is formatted for that particular application. A developer may wish to wait a long time before allowing the fall back defences to activate, thereby trapping infringer files and data which cannot be used without registering and paying for the application. IN certain cases, no such data is created and the developer may prefer a much shorter time before the fall back defences activate.

Overview

Figure 1 is a diagram showing a computer 100, and the Baitware software 104, acting on any number of software applications 102, within the computer.

Figure 2 shows the basic components of the system. A BaitwareLib.DLL file 200 is a compiled run time library containing a PCB, an RCR, and an instance of the Baitware class which contains Baitware instructions. An application executable file 202 contains any applications code, as well as a PCB instance. The computer registry 204 contains up to three instances of the RCR.

LockDef Record

The Lockdef record, shown in Figure 3, contains run time information, together with persistent data (preserved from one execution to the next). The data types shown as given in Microsoft MFC/C++. The top portion gives the set of input data, required during installation of an application. The next portions can be viewed as input or output, depending on the process involved. Lockdef forms the basis for most other records used in Baitware.

Program & Registry Control

With reference to Figure 4, the Program Control Block (PCB) 400 contains the set of data elements indicated in Figure 3. The Registry Control Record (RCR) 402 contains the indicated elements from LockDef 300, as well as an offset into the starting location of a PCB in the application executable file 202.

Constants

The different types for a LockDef occurrence are each represented by a different constant 404. Similarly, the different types of LockDef actions are also each represented by a different constant 406. Note that these constants are mutually inclusive and are therefore implemented as bit-flag values.

Member Duplication & Purpose

Figure.5 shows a table showing which data elements are duplicated in both the PCB and the RCR. This table also shows the purpose of each data member in each of the PCB and the RCR. The following notes apply to the superscripted numbers in Figure.5

(1) the RCR also contains additional members as shown in Figure.1

(2) hid is only required when the TLA_HELP action flag is supplied.

(3) url is only required when the TLA_CONNECT action flag is supplied.

Program File, Registry, and Record Associations

Figure 6 is a table showing the associations of each program file in the Baitware system with registry keys as well as with the PCB and RCR records. "<app><ver>.exe" is a self expanding archive with Baitware supporting code which immediately calls "setup.exe" after expansion is complete. "setup.exe" is a developer-generated setup program with Baitware supporting code which initially deletes the "<app><ver>.exe" file, then after installation is complete, it immediately activates the "app.exe" executable file. "app.exe" is the software

application being protected by Baitware which contains Baitware supporting code. The first action of "app.exe" is to delete the file "setup.exe".þ

Common Files for a Baitware Library

Figure 7 shows the files required for Baitware development. BaitwareLib.DLL 200 is a run-time library as described above; it must be located in a directory area such that the OS can find it (e.g. as part of a search path). BaitwareLib.LIB 700 is linked with an application to provide that application with Baitware supporting code. BaitwareLib.h 702 is a header file; this header must be included in in the application which wants to use BaitwareLib classes and functions. HexBuffer.h 704 is a header file; this header contains the declaration of the hex-key-string which is later burned-in with the PCB. It can be included in one and only one file of the application.þ

BurnIn

The "BurnIn" portion of the Baitware process is a developer tool kit which provides partial piracy protection for any application using a combination of the following information:

1) an Expiry time period and/or maximum number of executions.

2) a Machine Indentifier Value (MIV) which is automatically generated from the computer's characteristics.

3) User information; this is prompted for by the Burnin process according to developer-defined parameters.

All this information is saved (in encrypted form) in the following storage areas:

EXE-file. This is the .EXE file for the application. The data is written in developer defined locations, where each datum may be written at a different location. These locations provide immediate access to encrypted data buffers to any procedure in the application.

Burnin-file. This is a Burnin-definition file stored in the directory of the application. It contains encrypted data written at developer-defined locations. The rest of the file is filled in with random data.

Registry. The encrypted data is stored in the current system registry as data-values for developer-defined registry keys (or key-paths).

Using this information in the various locations, the BurnIn process can ensure the validity of the program being executed by the current user on the current computer.

The setup of the BurnIn module inside the application requires that certain steps be taken by which the application developer inserts and integrates the BurnIn module into his application (see Figure 8). Code is created 800 to test for the presence of the Baitware.DLL. Code is created 802 to ensure the HexBuffer.h file is present in at least one .CPP file in the application to be protected. Code is created

802 to properly link and align the applications project settings with the BaitwareLib.LIB file. The BaitwareLib.h file must be included 806 in all .CPP files. A call 808 to the BaitwareInit.h() must be inserted in the CXapp::Initinstance(). Code must be written 810 to create the BaitwareInit(), which module has the components shown in 812.

Once installed on the users system, BurnIn carries out a series of functions at every time when the application is run (Figure 9). These functions verify that the application is being run only on a valid system. Any and all errors result in the termination of the application. At the Start, verification is sought that the RegKey exists in the registry 900. If the HexKey is found, then the registry data is loaded and stored 902 in the RCR. Then the PCB offset in the .EXE file 904 is fetched the RCR. This permits the loading of the PCB data from the .EXE 706. If the RegKey is not found in 900, then an attempt is made to find the PCB in the .EXE file 908. If the HexKey is not found 910, then Error 02 error results 916 and the application terminates. If the HexKey is found 910, then the process proceeds to load the PCB data from the .EXE file and create the PCB 906. The process tests the PCB for validity 912 under two paths A/B. If not valid in either case the result is Error01 914 and the application terminates. Under path A, IsBurned() is tested 918 . If unsuccessful, the PCB and RCR are set 930 from the LockDef object values. The PCB is burned into the .EXE files 932. The RegKey is then created in the registry 934 and the values from the RCR are added. The process then tests to see if the RCR matches the PCB 926. If when the process tests for the IsBurned()

918, a return of YES results in Error03 920 . Under path B, the process again tests for IsBurned() 922. If unsuccessful, Error04 results 924 and the application terminates. If successful, the process matches the RCR with the PCB 926. A result of no gives rise to Error05 928 and the application terminates. A YES result brings the process to the Active Create module 936. A successful result leads to IsExpired() 938 and the End of the process. An unsuccessful result in Active Create also brings us to the end.

At the time of BurnIn, the fall back defenses can be installed in the .EXE using one or more drop dead dates. These dates are checked from time by the installed application and if reached would cause the application to fail loading (Figure 10). At the start, the burned application is initialized 1000. Failure to initialize gives rise to Error06 1002 and the application terminates. After successful initialization, the expiry date is checked 1004. If not expired, the process returns false 1006 and continues to run. If the application has expired then the RegTheUser module is activated 1008 to carry out a predetermined set of actions, which were specified by the developer. If the actions specified permits the application to continue, this is then the case 1010. If the specified actions are to terminate or to connect the user to the RIDSERVER, then the application terminates.

Baitware Errors

Figure 11 is a diagram showing the errors which are most likely to occur in the Baitware system. These error conditions 1100 are referenced throughout the

various process diagrams. Each error also has a probable cause 1102; the cause for any one error cannot be determined absolutely. The table 1102 lists the most probable causes.þ

Download to First Execution

Baitware works equally well for software downloaded from the Internet. Figure 12 shows the steps in such a process. First, the user downloads 1200 an executable archive from the Internet. Next, the user executes the downloaded file 1202 to expand and retrieve the files therein. This process involves the creation and validation of a Baitware object 1204, as well as the expansion of all files 1206 in that archive. The user has the option of canceling this process at any time 1222; however, at this point a user cancellation is too late since the Baitware validation process has already occurred. Next, the setup program (extracted from the archive) is automatically executed 1208. Again, this process involves the creation and validation of a Baitware object 1210, but this time the object is created and validated for the setup program. Once validated, the normal installation steps 1212 are undertaken. Again, the user may terminate the process at any time 1222. Upon the completion of the installation a dialog is displayed 1214, informing the user that installation is complete. Once the user presses the OK or CONTINUE button on this dialog, the software application is automatically executed 1216. Now a Baitware object is created and validated for the software application 1218. Finally, the software application can start its normal processing 1220; at this point, the application has been successfully encoded and validated via the Baitware process.þ

Registration-Identifier (RID)

Burnin presently incorporates user entered data (name and address) plus machine characteristics. The form which Burnin prompts a user is expanded to include a unique Registration Identifier (RID) which will be branded into the product together with the other information. The RID and the MIV can then be used as keys into the developer's customer database, to bind a RID (i.e. a copy of the product) directly to a user (an MIV).

The RID can be supplied to the customer in any way, including: adhesive label, printed sheet, and over the phone.

The RID is generated by the developer, starting at a base number (e.g. 0) and incrementally dispensed. A RID value is never re-used throughout the life-time of the application; it must remain unique across all copies of all versions of the application.

The RID Server

This solution envisions adding the RIDServer module to BurnIn. The RIDServer will run as a service on a designated station directly on a LAN (the Top Producer Hub); it will ensure that all executed copies of Top Producer are legitimate versions of the software.

Consider a customer with 20 computers on a LAN. The customer will receive a separate sheet, providing 20 different RID values. Now each station's MIV will be recorded either at installation time, or the first time Top Producer is executed from that station. All of the RID, MIV, and user-supplied data are maintained by the RIDServer in encrypted form. þ

Further, there is no central file or directory where all of the information is stored. Since the RIDServer will approve program access only for authorized computers (correct RID and correct MIV), the client is assured that as long as he does not give out the software, no one can access his private client information. Note that while the RIDServer must reside directly on the LAN, any station connected to the LAN, direct or via modem, can be checked for having the proper authorization.

The Baitware Process

The RID as used with Burnin allow for the Baitware method of software distribution/anti-piracy. Any means of software distribution can be used for Baitware. This ranges from mass-produced floppies and CD-ROMs to the Internet. The steps of the Baitware method are as follows:

1) Using the Burnin process described above, the application in version $V_{(x)}$ is released as "TrialWare" on date $D_{(x)}$; the application $V_{(x)}$ is BurnIned with the following information:

a) a trial period ($T_{(x)}$) from first execution, after which the program becomes expired. Depending on developer preference, expired programs are disabled via Burnin.

b) an undisclosed "absolute expiry date" or death-date, $D_{(d)}$, set for a date which is given by:

$D_{(d)} = D_{(x)} + T_{(d)}$, where $T_{(d)}$ is a time period of at least 3 times the time period $T_{(u)}$, as described by point 2).

c) a dynamically generated MIV.

d) user information (prompted for).

2) The Burnin process is augmented or enhanced with a new step to re-cover user-registration data from all installations and/or first-executions of the application. This step can be implemented in many forms.

The simplest is to print the registration form (including all user and dynamically generated data) with a mail-back address, then manually enter all data into a database.

The ideal way to implement this step is employ the RIDServer and transmit the registration data to it. The RIDServer maintains a database of all registered customers of the application. In this step, the RIDServer performs the following steps:

1. receive registration data packet,
2. decrypt registration data packet,

3. search database for matching RID,

4. if found

- Store all received information with the "infringer" tag in the database,
- Send back a negative response, indicating that the application should become expired,

5. else (if not found)

- Store all received information in the database; this means the process assumes that the user identified by the input MIV is now the legal owner of the application-copy identified by the input RID.

Note: if implemented as a simple mail-out-form, the steps outlined under the RIDServer would have to be manually performed by the developer.

Within a time period, $T_{(u)}$, after the release date, $D_{(x)}$, a free upgrade of the application in version $V_{(x+1)}$ is released. $T_{(u)}$ is specified by the developer as the time period required for the product to reach 50% of all illegal users. The upgrade $V_{(x+1)}$ will upgrade legal and illegal copies of the application in version $V_{(x)}$. The application $V_{(x+1)}$ will contain patches and responses to user requests. In addition, $V_{(x+1)}$ contains an encrypted list of all registered RID-MIV pairs, as extracted from the database constructed in step 2).

The following steps are performed during the Baitware Upgrade Process to weed out illegal users:

1. search the data base for a matching MIV-RID pair,

2. if found

- reset the absolute expiry date, $D_{(x)}$, to X years from current date; these are the authorized users or paid customers of the application (the reset-date is specified by the developer as the expected lifetime of the application in $V_{(x+1)}$),

3. else (if not found)

- if using a RIDServer, transmit all registration data. RIDServer will simply record all the data for later analysis,
- depending on developer preference, inform user that he/she is an illegal user of the application,
- leave the absolute expiry date, $D_{(x)}$, unchanged,

4. After the absolute expiry date, $D_{(d)}$, the infringer is faced with a situation where

- The installed application $V_{(x+1)}$ no longer works.

Pirating the upgrade $V_{(x+1)}$ does not help either, since the current machine's MIV must match. In fact, the upgrade can perform any action when a non-existing MIV is encountered, including disabling/deleting application data.þ

Baitware not only allows for mass CD-replication and Internet distribution, but also for a nearly full-proof way of preventing piracy.

Concise Restatements of the Invention

Primary Restatement

The primary restatement of the invention (in the most generic and general description) is that the developer can influence installed copies of his application remotely. By remotely, we mean where the developer does not know the physical location and/or ownership of some or all of the installed copies of the application which have been distributed to customers.

Secondary Restatement

A secondary restatement is that the developer can discriminate among those who would try to install the upgrades or updates based on features in his own customer database such as paid/unpaid, age, geographical location, etc. The developer can custom tailor each upgrade with a variety of approaches.

For example :

- Upgrade feature A (say the removal of a drop dead date)- paid users only.
- Up grade feature B (all users, regardless of paid unpaid status)
- UF - C - All valid MIVs of odd number
- UF - D - All valid MIVs of even number
- UF - E - All MIVs of even number
- UF - F - All MIVs of odd number

The choice of odd and even was for purpose of illustration. The developer choose to sort his customer database in some fashion and the upgrades (and hence

his ability to remotely influence each and every copy of the installed base, without having to know where it was located or in whose possession it was stored applies.

It is not the purpose of this method to apply a value judgement on what basis a developer might choose to discriminate among those using his application.

The above description is not intended to limit the claimed invention in any manner, furthermore, the discussed combination of features might not be absolutely necessary for the inventive solution.

The present invention has been described with regard to preferred embodiments. However, it will be obvious to persons skilled in the art that a number of variations and modifications can be made without departing from the scope of the invention as described herein.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OF PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1.) The present invention comprises a method and means of preventing software piracy whereby software is treated and distributed according to the Baitware process; the Baitware process comprising the steps of:

a.)Treating the software to use the Burnin process, wherein Burnin performs the initialization steps of:

i.)Calculating a trial period ($T_{(x)}$) from first execution, after which the program becomes expired, whereby expired programs are disabled via Burnin depending on software developer preference,

ii.)Assigning an undisclosed "absolute expiry date" or death-date, $D_{(d)}$, set for a date which is given by:

$D_{(d)} = D_{(x)} + T_{(d)}$, where $T_{(d)}$ is a time period of at least 3 times the time period $T_{(u)}$

iii.)Dynamically generating an MIV value using the current computer software and hardware configurations,

iv.)Prompting the user for user information and the developer supplied RID, where the set of user information is specified by the software developer,

v.)Recording all data from steps i-iv in random and developer-specified locations in the executable file for the software,

vi.)Recording all data from steps i-iv in random and developer-specified locations within the current system-configuration-definition or registry,

b.)Distributing the BurnIned software in version $V_{(x)}$ as TrialWare on the date $D_{(x)}$ via any and all distribution channels, these channels including:

i.)Floppies

ii.) CD-ROM

iii.) Internet

iv.) Intranet

v.)Extranet

c.)Generating and dispensing a new and unique RID value for each copy of software sold to a user, the RID value being unique across all versions of the software throughout its life-time,

d.)Augmenting the Burnin process with a new step to re-cover user-registration data for paid users, including the MIV and RID values, from all installations and/or first-executions of the software, and to further store this data in the Customer Database,

e.)Constructing a free upgrade of the software in version $V_{(x-1)}$ which includes the Customer Database constructed in step d; version $V_{(x+1)}$ being able to upgrade legal and illegal copies of the software in version $V_{(x)}$ via the initialization steps of:

i.)Searching the Customer Database for a matching MIV-RID pair,

ii.)If found, resetting the absolute expiry date, $D_{(x)}$, to Y years from current date, where Y is defined as the life-time of the software in version $V_{(x+1)}$,

iii.)If not found, recording all registration data and dynamically generated data to the central data base of step d, identifying a particular MIV as an illegal, but still upgraded user,

f.)Distributing the software in version $V_{(x+1)}$ constructed in step-e as a free upgrade within a time period, $T_{(u)}$, after the release date, $D_{(x)}$, where $T_{(u)}$ is specified by the software developer as the time period required for the product to reach 100% of currently legal users,

g.)Disabling each copy of the software in version $V_{(x+1)}$ on the death date $D_{(d)}$; this process, which is activated the next time the software is run on or after the death date, comprising the steps of:

i.)Executing and/or undertaking all additional actions specified by the software developer,

ii.)Further disabling the software in version $V_{(x)}$, thereby also disabling any future re-installations of the software in version $V_{(x)}$,

h.)Contacting all illegal users recorded in the Customer Database on the death date $D_{(d)}$, and communicating all software developer specified information.

2. A method and means of software distribution and re-distribution whereby software piracy is eliminated; the process comprising the same steps as 1 above.

3. A method and means of preventing software piracy wherein the released software is protected from infringement by forcing infringers to have to register the software product for continued use.

4. A method and means of preventing software piracy wherein infringers of released software are coerced into purchasing the product for continued use.

5. A method and means of preventing software piracy as in 1 above, wherein each dynamically generated MIV value (1.x) is further associated with user information consisting of the following data:

a.)Name,

b.)Email,

c.)Address,

d.)Phone,

e.)etc.

6. A method and means of preventing software piracy as in 5 above, where the released and branded software (1.x) is further used to distinguish paying users from infringers, such that an infringer's copy of the software also identifies the paying user who illegally re-distributed the software.

7. A method and means of preventing software piracy wherein new market share for the software is forcibly created from the illegal user market for that software.

8. A method and means of preventing software piracy wherein new marketing and distribution channels are forcibly created from the illegal distribution channels for that software.

9. A method and means of preventing software piracy as in 1 above, wherein Copying the installed application from one legal machine to an infringer (even if the registry information is correctly updated) will not enable the infringer to run the application, since the program will generate a different MIV from that which has been burned into its own executable.

10. A method and means of enforcing the terms of any software license by controlling any copy of software after it has left the actual possession of the developer.

11. A method and means of creating a database for maintaining ongoing customer relations.

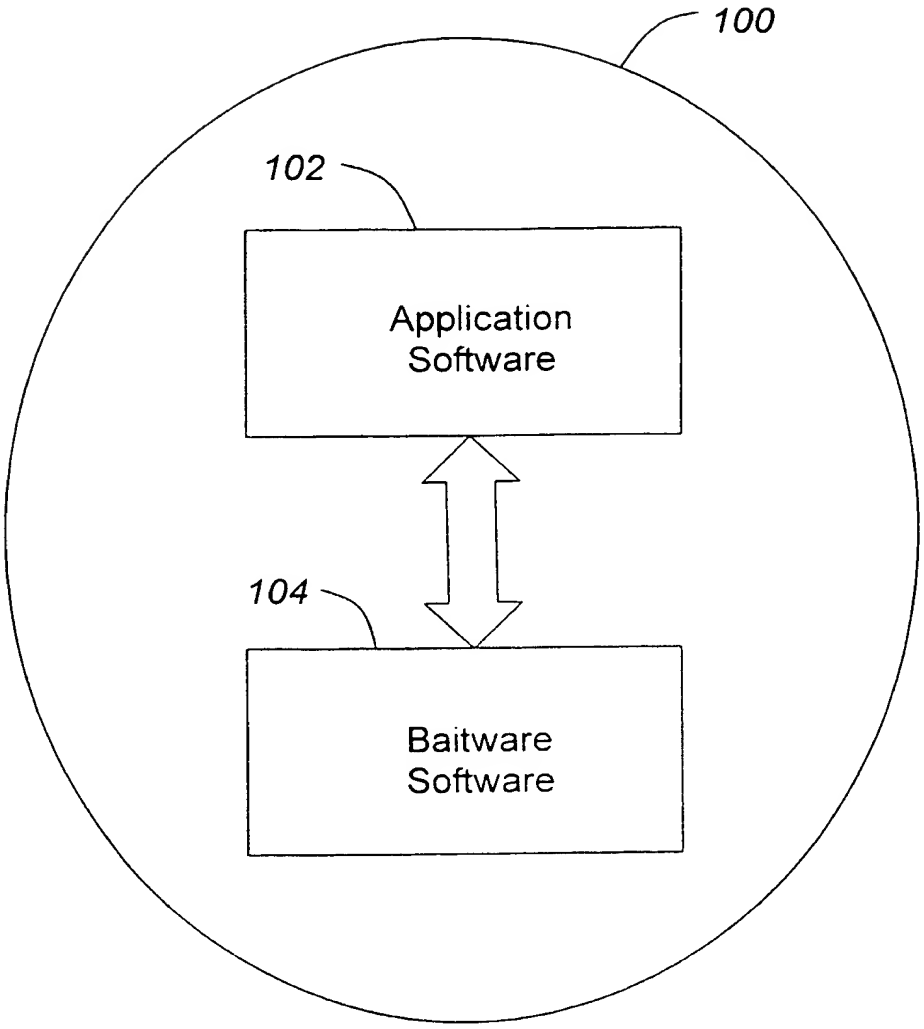

FIG. 1

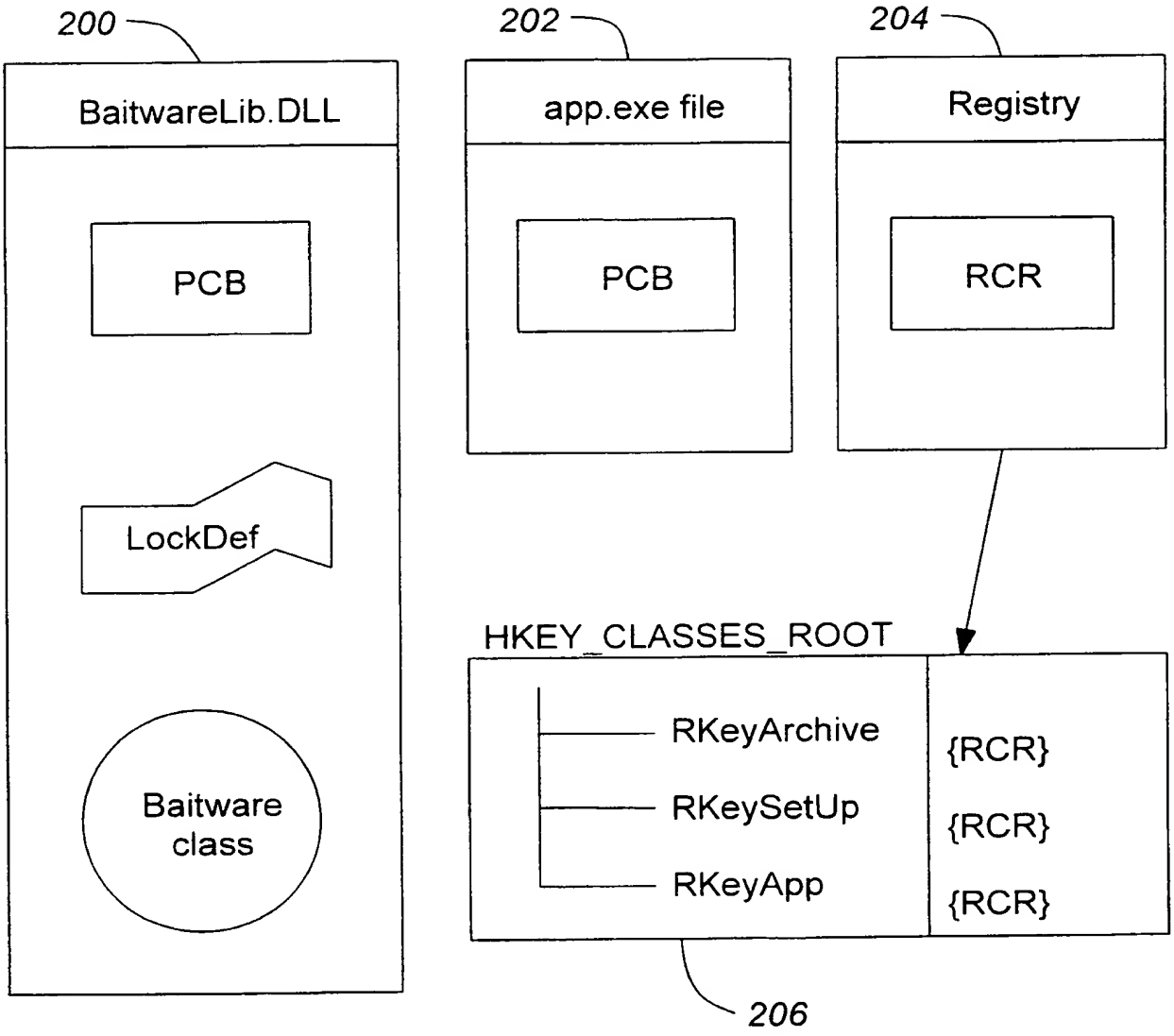
200
BaitwareLib.DLL
PCB
LockDef
Baitware class
202
app.exe file
PCB
204
Registry
RCR
HKEY_CLASSES_ROOT
RKeyArchive
RKeySetUp
RKeyApp
{RCR}
{RCR}
{RCR}
206

FIG. 2

300

```
LockDef
//REQUIRED INPUT (these members also occur in the PCB)
UEI             idProg;         //used to create subKeys; a GPID_*value
BITMASK         type;           //date types (TLT_*values)
BITMASK         action;         //action types (TLA_*values)
CTimeSpan       period;         //an expiry period
CTime           date;           //an expiry date
UINT            hid;            //help ID to display
CString         url;            //URL to file or site

//OPTIONAL INPUT OR OUTPUT (these members also occur in the PCB)
int             graceDays;      //number of days to run after expiry; TLA_GRACE must be set
CString         regKey;         //auto or program-supplied key-name for registry; when not
                                //supplied as input, the default name is output in this member
CString         progName;       //name of application which made the call
CString         company;        //company copyright/name of applicator which made the call

//OPTIONAL INPUT OR OUTPUT (these members do NOT occur in the PCB)
UINT*           hexKey;         //program supplied hex-key to search for in the .EXE file
                                //when not supplied as input, the default hex-key is assumed

//PERSISTENT OUTPUT (these members also occur in the PCB)
/ctime          tmExpire;       //serialized expiry date value

//RUN-TIME OUTPUT (these members do NOT occur in the PCB)
HKEY            hkey;           //open registry handle for a program's key
Int             selection;      //user selected action value; one of the TLA_*values
PCB*            pcb;            //allocated PCB as loaded from .EXE file
```

FIG. 3

Program Control block (PCB) 400

```
//same members as LockDef, except
//for each CString member we have a static UINT array
//only the indicated members of LockDef are duplicated in the PCB
//the members are NOT included in the same order
```

FIG. 4

Registry Control Record (RCR) 402

```
//this type contains all LockDef members designated
//or the registry, it also includes:
OFFSET    offPCB;    //previously found offset of PCB in the .EXE file
```

Time Lock Type (TLT) constants for LockDef. type 404

```
//INPUT
#define TLT_FIXED_DATE          0x0001    //Program expires on a fixed date
#define TLT_TIME_PERIOD         0x0002    //Program expires after a fixed period, after first execution
#define TLT_NO_ACTION           0x0004    //on expiry do not take action;return action value(s);debugging only
#define TLT_ACTIVE_CREATE       0x0008    //after Baitware creation;automatically calls IsExpired();default;off
//OUTPUT
#define TLT_EXPIRED             0x8000    //indicates the expiry date has been reached
```

Time Lock Action (TLA) constants for LockDef.action 406

```
#define TLA_HELP                0x0001    //make a help button available
#define TLA_CONTINUE            0x0002    //if this flag is on, a continue button is available
#define TLA_CONNECT             0x0004    //make a connect button available
#define TLA_QUIT                0x0008    //defined to complete return-value set
#define TLA_REMAINING           0x0010    //always display dialog w/ remaining days to expiry
#define TLA_GRACE               0x0020    //allow execution for LockDef.graceDays days after expiry
```

MEMBER		*INPUT*	*OUTPUT*	*PCB*	*RCR(1)*
UEI	idProg	REQUIRED	NO	YES	YES
BITMASK	type	REQUIRED	NO	YES	NO
CTimeSpan	period	REQUIRED	NO	YES	NO
CTime	date	REQUIRED	NO	YES	NO
UINT	hid	REQUIRED(2)	NO	YES	NO
CString	url	REQUIRED(3)	NO	YES	NO
CString	regKey	OPTIONAL	YES	YES	NO
CString	progName	OPTIONAL	YES	YES	YES
CString	company	OPTIONAL	YES	YES	YES
UINT*	hexKey	OPTIONAL	YES	NO	NO
Ctime	tmExpire	NO	YES	YES	YES
HKEY	hkey	NO	YES	NO	NO
int	selection	NO	YES	NO	NO
PCB*	pcb	NO	YES	NO	NO

FIG. 5

Program	*Registry Key Variable*	*Actual Registry Key Name*	*Registry Key Values*	*Data Burned-In Program*
<app><ver>.exe	RKeyArchive	<val. passed by Archive>	RCR	PCB
setup.exe	RKeySetup	<value passed by Setup>	RCR	PCB
<app>.exe	RKeyApp	<value passed by App>	RCR	PCB

FIG. 6

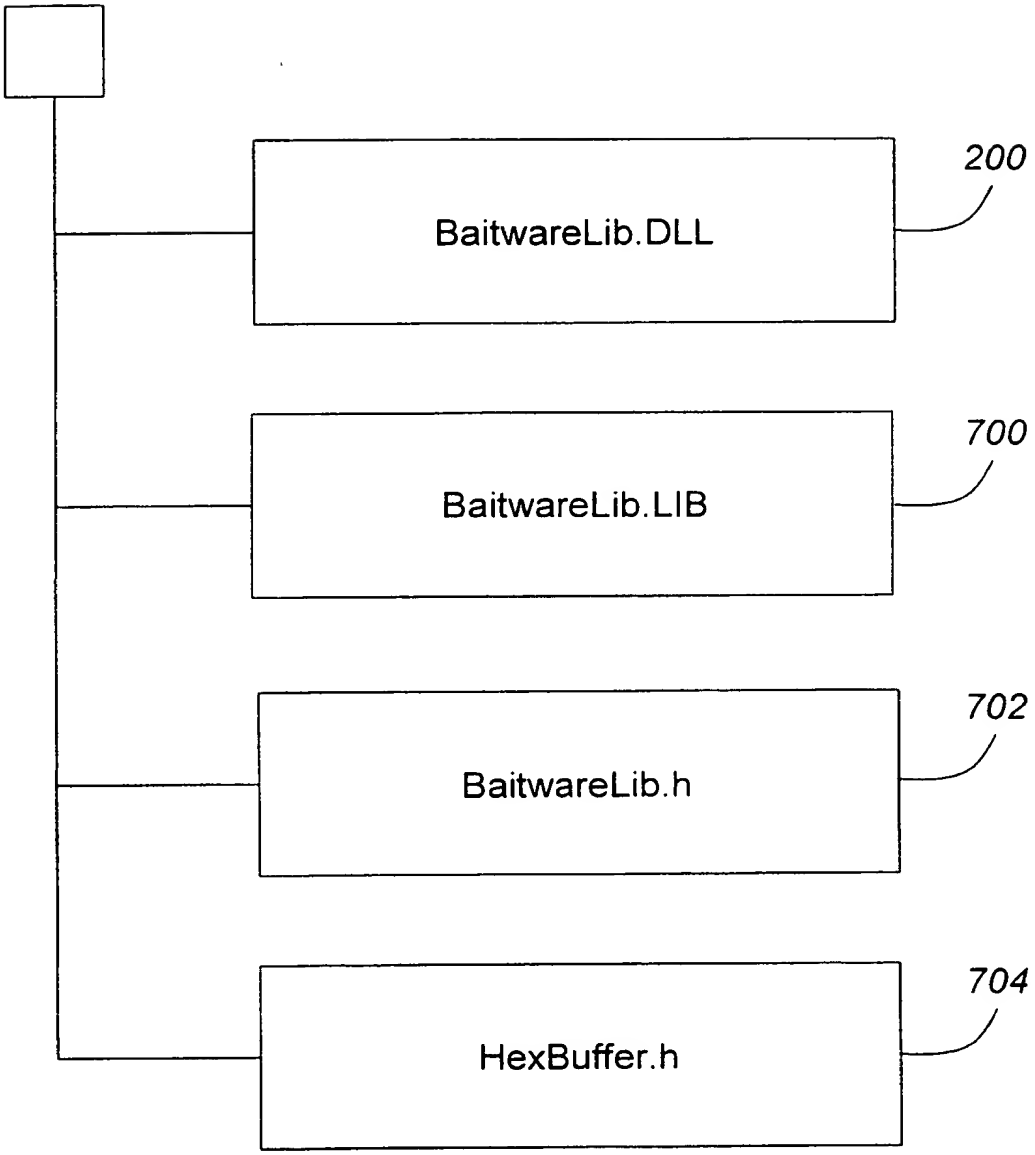
BaitwareLib.DLL
200
BaitwareLib.LIB
700
BaitwareLib.h
702
HexBuffer.h
704

FIG. 7

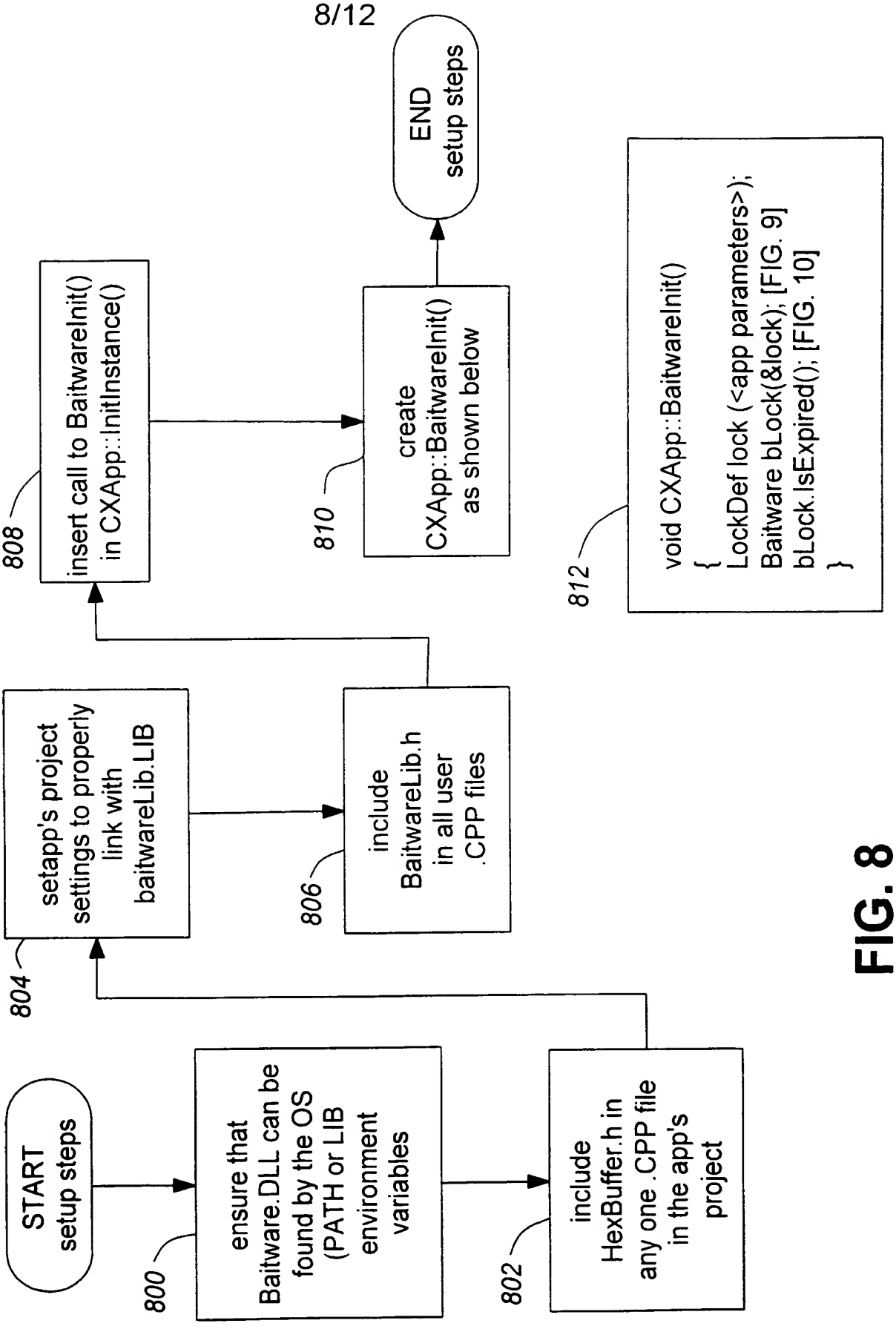
START
setup steps
ensure that Baitware.DLL can be found by the OS (PATH or LIB environment variables
include HexBuffer.h in any one .CPP file in the app's project
setapp's project settings to properly link with baitwareLib.LIB
include BaitwareLib.h in all user .CPP files
insert call to BaitwareInit() in CXApp::InitInstance()
create CXApp::BaitwareInit() as shown below
END
setup steps
void CXApp::BaitwareInit()
{
LockDef lock (<app parameters>);
Baitware bLock(&lock); [FIG. 9]
bLock.IsExpired(); [FIG. 10]
}
800
802
804
806
808
810
812

FIG. 8

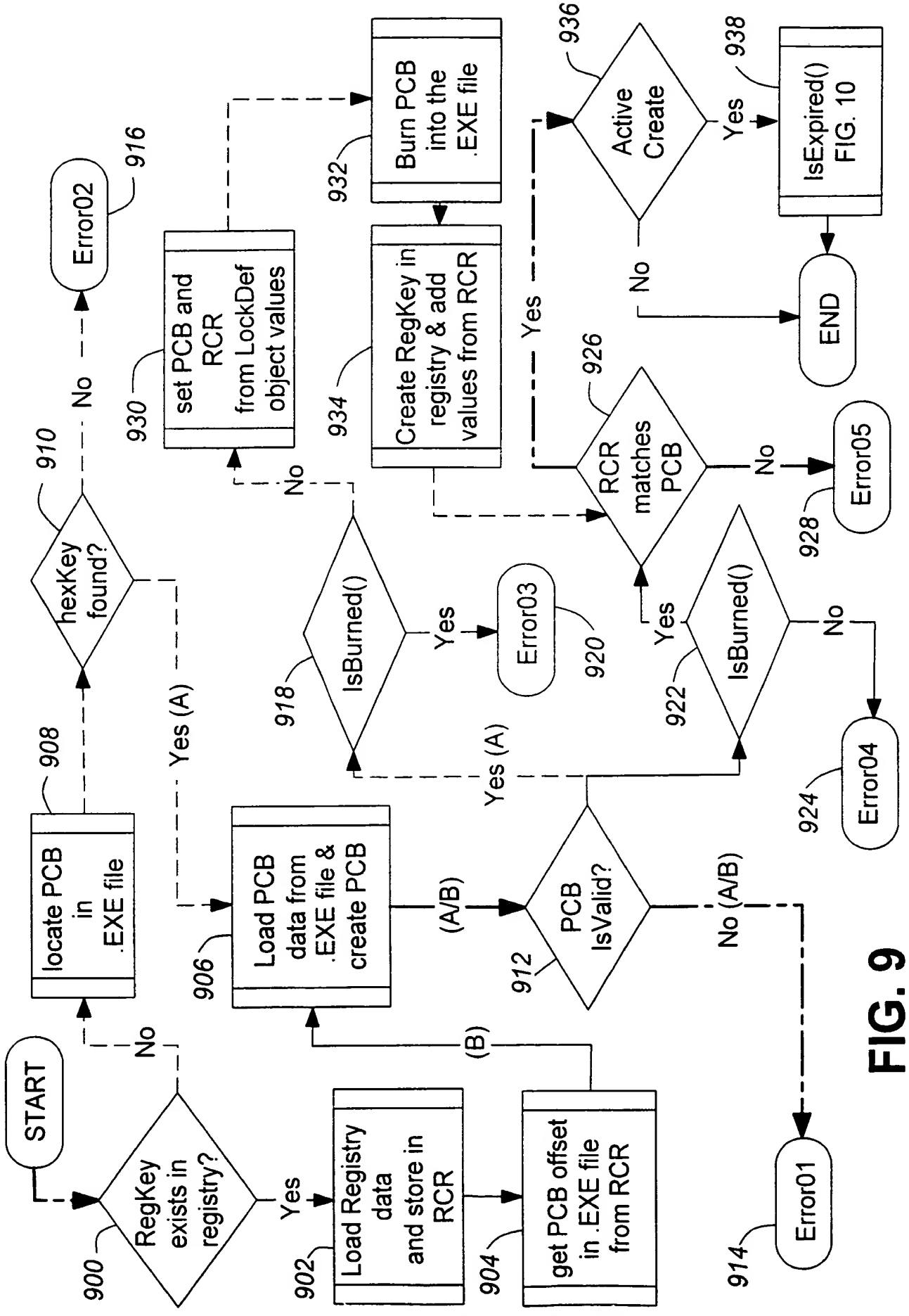
START
RegKey exists in registry?
900
No
Yes
Load Registry data and store in RCR
902
get PCB offset in .EXE file from RCR
904
(B)
Load PCB data from .EXE file & create PCB
906
(A/B)
PCB IsValid?
912
No (A/B)
Error01
914
Yes (A)
locate PCB in .EXE file
908
hexKey found?
910
No
Error02
916
Yes (A)
IsBurned()
918
Yes
Error03
920
No
set PCB and RCR from LockDef object values
930
Burn PCB into the .EXE file
932
Create RegKey in registry & add values from RCR
934
IsBurned()
922
Yes
No
Error04
924
RCR matches PCB
926
No
Error05
928
Yes
Active Create
936
Yes
IsExpired() FIG. 10
938
No
END

FIG. 9

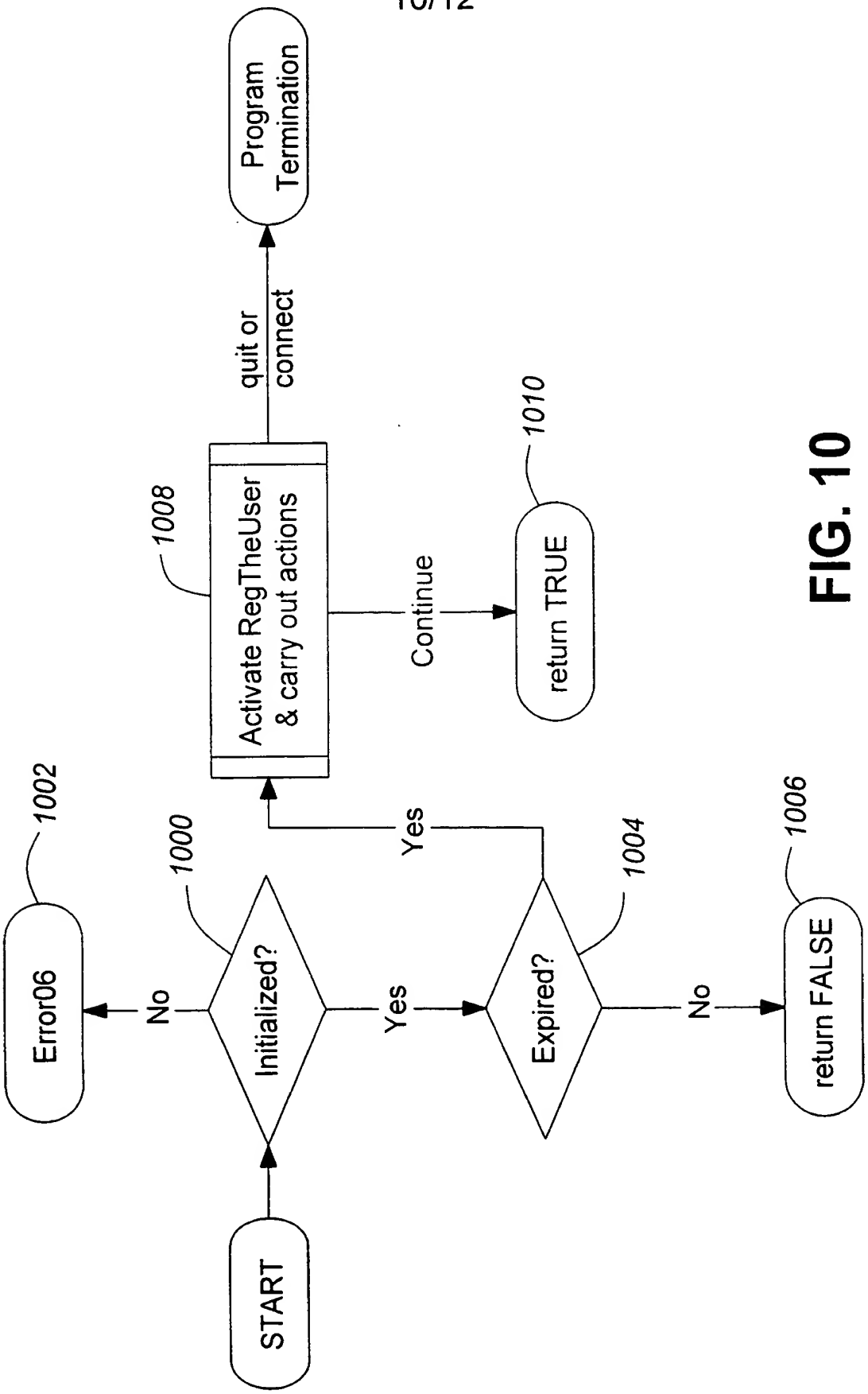
START
Initialized?
1000
Error06
1002
No
Yes
Expired?
1004
return FALSE
1006
Yes
Activate RegTheUser & carry out actions
1008
Continue
return TRUE
1010
quit or connect
Program Termination

FIG. 10

No.	Description of Condition	Possible Cause(s)
01	The program's PCB is invalid	A
02	Hex key not found in .EXE file	A
03	There was no registry key found, but the .EXE file was burned-in	B,C
04	Registry key(s) exist, but the .EXE file is not burned-in	D,C
05	The program's PCB does match the RCR in the registry	B,C,D
06	IsExpired called but Baitware is not initialized	E

1100

Cause-ID	Possible Cause of Condition
A	.EXE file for program is invalid or corrupted
B	Registry tampering by user
C	Partially completed uninstall or re-install
D	User previously saved .EXE file and has now copied over installed version
E	Programmer error; the program using Baitware is not initializing the object properly

1102

FIG. 11

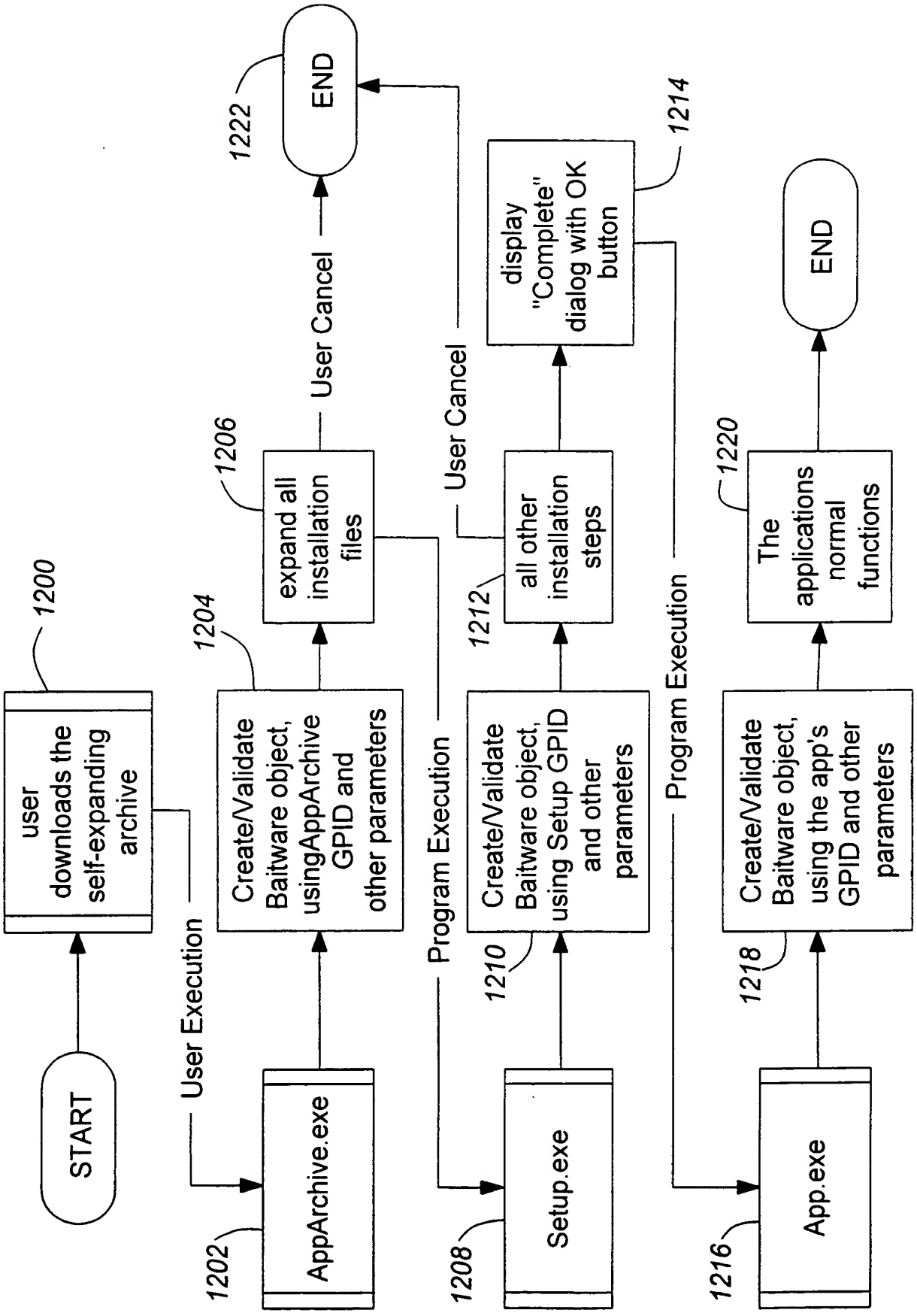
START
AppArchive.exe
1202
User Execution
user downloads the self-expanding archive
1200
Create/Validate Baitware object, usingAppArchive GPID and other parameters
1204
expand all installation files
1206
User Cancel
END
1222
Setup.exe
1208
Program Execution
Create/Validate Baitware object, using Setup GPID and other parameters
1210
all other installation steps
1212
User Cancel
display "Complete" dialog with OK button
1214
App.exe
1216
Program Execution
Create/Validate Baitware object, using the app's GPID and other parameters
1218
The applications normal functions
1220
END

FIG. 12

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 99/00560

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 94 07204 A (R. RICHARDSON) 31 March 1994 (1994-03-31) page 1, line 8 -page 10, line 10 page 12, line 6 -page 23, line 9; claims; figures 1-8	1-3,11
A	EP 0 679 980 A (I. B. M.) 2 November 1995 (1995-11-02) column 8, line 47 -column 17, line 56; figure 15	1,5,9
A	US 5 291 598 A (GRUNDY) 1 March 1994 (1994-03-01) column 1, line 16 -column 6, line 23; claim 1; figure 1A	1-3,11

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 October 1999	20/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Soler, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 99/00560

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9407204 A	31-03-1994	AU 678985 B	19-06-1997
		AU 4811393 A	12-04-1994
		CA 2145068 A	31-03-1994
		CN 1103186 A	31-05-1995
		EP 0689697 A	03-01-1996
		NZ 255971 A	26-05-1997
		US 5490216 A	06-02-1996
EP 679980 A	02-11-1995	US 5757907 A	26-05-1998
		BR 9501522 A	21-11-1995
		CA 2145926 A,C	26-10-1995
		JP 7295801 A	10-11-1995
US 5291598 A	01-03-1994	US 5375240 A	20-12-1994